

1 KEKER & VAN NEST, LLP  
JOHN W. KEKER - #49092  
2 MICHAEL H. PAGE - #154913  
710 Sansome Street  
3 San Francisco, CA 94111-1704  
Telephone: (415) 391-5400  
4 Facsimile: (415) 397-7188

5 DERWIN & SIEGEL, LLP  
DOUGLAS K. DERWIN - #111407  
6 3280 Alpine Road  
Portola Valley, CA 94028  
7 Telephone: (408) 855-8700  
Facsimile: (408) 529-8799

8 INTERTRUST TECHNOLOGIES CORPORATION  
9 MARK SCADINA - #173103  
JEFF MCDOW - #184727  
10 4800 Patrick Henry Drive  
Santa Clara, CA 95054  
11 Telephone: (408) 855-0100  
Facsimile: (408) 855-0144

12 Attorneys for Plaintiff and Counter-Defendant  
13 INTERTRUST TECHNOLOGIES CORPORATION

14  
15 UNITED STATES DISTRICT COURT  
16 NORTHERN DISTRICT OF CALIFORNIA  
17

18 INTERTRUST TECHNOLOGIES  
CORPORATION, a Delaware corporation,

19 Plaintiff,

20 v.

21 MICROSOFT CORPORATION, a  
22 Washington corporation,

23 Defendant.

24 AND COUNTER ACTION.  
25  
26  
27  
28

Case No. C 01-1640 SBA (MEJ)

Consolidated with C 02-0647 SBA

**INTERTRUST'S OPENING CLAIM  
CONSTRUCTION BRIEF**

Date: May 12, 29, & 30, 2003  
Time: 9:00 a.m.

# TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION .....	1
II. FACTUAL BACKGROUND .....	2
III. CLAIM CONSTRUCTION PRINCIPLES IN GENERAL .....	3
IV. THE LENGTH AND COMPLEXITY OF MICROSOFT'S PROPOSED CONSTRUCTIONS .....	5
V. SPECIFIC CLAIM CONSTRUCTION ISSUES .....	6
A. Global Requirement of a Virtual Distribution Environment (Ex. A, Row 1, Ex. B, Row 24, Ex. C, Tab 24).....	7
1. The eleven claims other than 900.155 do not recite a "Virtual Distribution Environment" and do not contain any language implying any such requirement.....	7
2. Incorporation of Virtual Distribution Environment into Claims Neither Reciting Nor Implying Such a Limitation Is Improper.....	8
a. The eleven claims other than 900.155 contain no limitations relating to a Virtual Distribution Environment.....	9
b. Statements in the specifications do not clearly disclaim patentable subject matter, and therefore cannot be used to limit the claims.....	9
c. Specification statements about the "invention" are only one factor in claim interpretation, and must be interpreted in light of the entire specification and file history. ....	10
(i) The Patent Office ruled that the parent InterTrust patent application involved five separate and independent classes of invention.....	11
(ii) Microsoft's interpretation of "the invention" is contradicted by the claims. ....	13
B. Secure/Security (Ex. A, Row 3, Ex. B, Row 19, Ex. C, Tab 19).....	14
C. Budget (Ex. A, Row 4, Ex. B, Row 3, Ex. C, Tab 3). ....	16
D. Control (noun) (Ex. A, Row 4, Ex. B, Row 8, Ex. C, Tab 8). ....	17
E. Copy/Copied/Copying (Ex. A, Row 5, Ex. B, Row 10, Ex. C, Tab 10).....	19
F. Budget Specifying the Number of Copies Which Can Be Made of Said Digital File (Ex. A, Row 6, Ex. B, Row 25, Ex. C, Tab 25).....	21

**TABLE OF CONTENTS**  
(cont'd)

	<u>Page</u>
G. Control (verb) (Ex. A, Row 7, Ex. B, Row 9, Ex. C, Tab 9).....	21
H. Controlling the Copies Made of Said Digital File (Ex. A, Row 7, Ex. B, Row 26, Ex. C, Tab 26).....	22
I. Authentication (Ex. A, Row 27, Ex. B, Row 2, Ex. C, Tab 2).....	23
J. Identifier (Ex. A, Row 28, Ex. B, Row 17, Ex. C, Tab 17).....	24
K. Clearinghouse (Ex. A, Row 40, Ex. B, Row 4, Ex. C, Tab 4).....	25
L. Use (Ex. A, Row 42, Ex. B, Row 23, Ex. C, Tab 23).....	25
M. Secure Container (Ex. A, Row 57, Ex. B, Row 20, Ex. C, Tab 20).....	26
N. Contain/Containing (Ex. A, Row 58, Ex. B, Row 7, Ex. C, Tab 7).....	27
O. Aspect (Ex. A, Row 60, Ex. B, Row 1, Ex. C, Tab 1).....	28
P. Protected Processing Environment (Ex. A, Row 62, Ex. B, Row 18, Ex. C, Tab 18).....	28
Q. Digital Signature/Digitally Signing (Ex. A, Row 66, Ex. B, Row 14, Ex. C, Tab 14).....	30
R. Designating (Ex. A, Row 66, Ex. B, Row 12, Ex. C, Tab 12).....	30
S. Device Class (Ex. A, Row 66, Ex. B, Row 13, Ex. C, Tab 13).....	31
T. Tamper Resistance (Ex. A, Row 67, Ex. B, Row 21, Ex. C, Tab 21).....	31
U. Digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class (Ex. A, Row 67, Ex. B, Row 27, Ex. C, Tab 27).....	32
V. Tamper Resistant Barrier (Ex. A, Row 71, Ex. B, Row 22, Ex. C, Tab 22).....	32
W. Executable Programming/Executable (Ex. A, Row 73, Ex. B, Row 15, Ex. C, Tab 15).....	33
X. Securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item (Ex. A, Row 85, Ex. B, Row 28, Ex. C, Tab 28).....	34
Y. Virtual Distribution Environment (Ex. A, Row 86, Ex. B, Row 24, Ex. C, Tab 24).....	35

TABLE OF CONTENTS  
(cont'd)

	<u>Page</u>
Z. Host Processing Environment (Ex. A, Row 87, Ex. B, Row 16, Ex. C, Tab 16).....	36
AA. Derive (Ex. A, Row 92, Ex. B, Row 11, Ex. C, Tab 11).....	37
BB. Derives information from one or more aspects of said host processing environment (Ex. A, Row 92, Ex. B, Row 29, Ex. C, Tab 29).....	37
CC. Compares/Comparison (Ex. A, Row 94, Ex. B, Row 5, Ex. C, Tab 5).....	38
DD. Component Assembly (Ex. A, Row 99, Ex. B, Row 6, Ex. C, Tab 6).....	38
EE. Identifying at least one aspect of an execution space required for use and/or execution of the load module (Ex. A, Row 103, Ex. B, Row 30, Ex. C, Tab 30).....	39
VI. CONCLUSION.....	40

# TABLE OF AUTHORITIES

Page(s)

## FEDERAL CASES

<i>Alfred J. Schumer v. Laboratory Computer Systems, Inc.</i> , 308 F.3d 1304 (Fed. Cir. 2002) .....	35
<i>Altiris, Inc. v. Symantec Corp.</i> , 318 F.3d 1363 (Fed. Cir. 2003) .....	35
<i>Amgen Inc. v. Hoechst Marion Roussel, Inc.</i> , 314 F.3d 1313 (Fed. Cir. 2003) .....	9, 10
<i>Control Resources, Inc. v. Delta Electronics, Inc.</i> , 133 F. Supp. 2d 121 (D. Mass. 2001) .....	6
<i>Ecolab, Inc. v. Envirochem, Inc.</i> , 264 F.3d 1358 (Fed. Cir. 2001) .....	10
<i>Honeywell Inc. v. Victor Co. of Japan, Ltd.</i> , 298 F.3d 1317 (Fed. Cir. 2002) .....	10
<i>Laitram Corp. v. Cambridge Wire Cloth Co.</i> , 863 F.2d 855 (Fed. Cir. 1988), <u>cert. denied</u> , 490 U.S. 1068 (1989) .....	17
<i>MacNeill Engineering Co., Inc. v. Trisport, Ltd.</i> , 126 F. Supp. 2d 51 (D. Mass. 2001) .....	6
<i>Markman v. Westview Instruments, Inc.</i> , 517 U.S. 370 (1996) .....	3
<i>McCarty v. Lehigh Valley R.R.</i> , 160 U.S. 110 (1895) .....	4
<i>McGinley v. Franklin Sports, Inc.</i> , 262 F.3d 1339 (Fed. Cir. 2001) .....	13
<i>Moore U.S.A., Inc. v. Standard Register Co.</i> , 229 F.3d 1091 (Fed. Cir. 2000), <u>cert. denied</u> , 532 U.S. 1008 (2001) .....	10
<i>Rambus Inc. v. Infineon Techs. Ag.</i> , 318 F.3d 1081 (Fed. Cir. 2003) .....	11, 13
<i>Renishaw PLC v. Marposs Societa' per Azioni</i> , 158 F.3d 1243 (Fed. Cir. 1998) .....	4, 9
<i>SKW Americas v. Euclid Chemical Co.</i> , 231 F. Supp. 2d 626 (N.D. Ohio 2002) .....	6
<i>SRI International v. Matsushita Electric Corp. of America</i> , 775 F.2d 1107 (Fed. Cir. 1985) .....	4
<i>Teleflex, Inc. v. Ficosa North America Corp.</i> , 299 F.3d 1313 (Fed. Cir. 2002) .....	10
<i>Texas Digital Systems, Inc. v. Telegenix, Inc.</i> , 308 F.3d 1193 (Fed. Cir. 2002) .....	3, 4, 5
<i>Transco Products, Inc. v. Performance Contracting</i> , 38 F.3d 551 (Fed. Cir. 1994), <u>cert. denied</u> , 513 U.S. 1151 (1995) .....	12

TABLE OF AUTHORITIES  
(cont'd)

Page(s)

*Vitronics Corp. v. Conceptronic, Inc.*,  
90 F.3d 1576 (Fed. Cir. 1996) .....31

**FEDERAL STATUTES**

35 U.S.C. § 112.....4

35 U.S.C. § 121.....11

1 I. INTRODUCTION

2 This case pits a small, innovative industry pioneer against a monopolistic giant whose  
3 ruthless, anticompetitive tactics are legendary. InterTrust invented the field of Digital Rights  
4 Management ("DRM"). Microsoft praised InterTrust's work as revolutionary, negotiated with  
5 InterTrust for a license to InterTrust's technology and patents, then broke off negotiations and  
6 unilaterally designed InterTrust's innovations into a large portion of Microsoft's product line.

7 InterTrust, however, has one asset Microsoft's other victims did not possess: long before  
8 Microsoft had even heard of Digital Rights Management, InterTrust filed foundational patents in  
9 the field, patents that now read directly on major Microsoft initiatives in this area.

10 Microsoft now seeks to avoid the consequences of its actions by urging this Court to  
11 adopt claim constructions that would render the InterTrust claims meaningless. Microsoft would  
12 have this Court read a single, two thousand word definition into every single InterTrust claim, a  
13 definition at least twenty times longer than any claim construction ever adopted by any Court,  
14 and almost certainly far longer than any definition ever even proposed. No jury could possibly  
15 comprehend Microsoft's two thousand word definition, much less apply it in any meaningful  
16 way.

17 Nor could any jury meaningfully apply numerous other claim construction proposals  
18 from Microsoft, many of which amount to hundreds of words of highly complicated text.  
19 Microsoft's constructions improperly read dozens of detailed limitations from specification  
20 embodiments into the claims and incorporate numerous other restrictions that contradict the  
21 specifications or are made up from whole cloth. Microsoft's proposed definitions are  
22 inconsistent with fundamental canons of claim construction.

23 By contrast, InterTrust's straightforward claim constructions conform to the plain  
24 language of the claims, informed by the specifications, and provide a clear and informative  
25 blueprint that can easily be understood and applied by the trier of fact. That a straightforward  
26 approach compels a finding of infringement may not be to Microsoft's liking, but it is what the  
27 law requires.

28

1    **II.     FACTUAL BACKGROUND**

2           The InterTrust patents involved in this litigation derive from a foundational patent  
3 application filed in February 1995. That application resulted from a number of years of  
4 concentrated work by the four inventors, starting with an investigation first begun by InterTrust  
5 founder Victor Shear in the 1980s.<sup>1</sup> From InterTrust's inception in 1990 and throughout the  
6 following decade, Mr. Shear and his colleagues tackled the most intractable difficulties  
7 confronting the digital marketplace: how to enable authors, publishers, and other owners of  
8 digital content to distribute and sell that content electronically, while simultaneously protecting  
9 that content from misuse and piracy. InterTrust not only saw the problems that currently plague  
10 electronic commerce, it discovered crucial solutions, and then described those solutions in the  
11 patents that are the subject of this claim construction brief.

12           The foundational InterTrust patent application describes an overall "architecture" for  
13 Digital Rights Management, an integrated approach designed for conducting trusted and secure  
14 electronic commerce.<sup>2</sup> InterTrust's inventors began thinking about these concepts long before  
15 the rest of the computer industry, and literally years before Microsoft had given any thought  
16 whatsoever to DRM.

17           InterTrust's design and approach were widely recognized in the industry as  
18 groundbreaking and revolutionary. For example, one senior Microsoft executive was quoted as  
19 follows:

20           "InterTrust is solving problems that won't be in the mainstream for quite some  
21 time," says Will Poole, senior director of marketing and business development at  
22 Microsoft's Streaming Media Division. "It's visionary."

23           The Wall Street Journal, April 29, 1999, Page Decl. Exh. A. The InterTrust patents were also  
24 recognized in the industry as fundamental: "'Before anybody had thought about this stuff,  
25 [Victor Shear] was out there patenting it,' said Kirk Loevner, a former Apple Computer Inc.

26           <sup>1</sup> See Declaration of Michael Page ("Page Decl."), Exh. A, for a more detailed history of  
27 InterTrust. See also Shear Deposition Transcript 157:13-158:23 (Page Decl., Exh U);  
28 Supplemental Response of Plaintiff InterTrust Technologies Corp. to Defendant Microsoft  
Corporation's First Set of Interrogatories (Page Decl., Exh. V).

<sup>2</sup> See Declaration of Dr. Michael Reiter ("Reiter Decl."), ¶¶ 10-15.



1 executive.” Id.

2 Starting in 1998, Microsoft negotiated for a license to InterTrust’s technology and  
3 patents. These negotiations involved literally dozens of meetings, at which InterTrust made  
4 significant disclosure of its technical architecture. In 2000, Microsoft terminated these  
5 discussions. In the same timeframe, Microsoft announced its .NET initiative, a major Microsoft  
6 project designed to incorporate DRM into all aspects of Microsoft’s products. This lawsuit  
7 followed.

### 8 III. CLAIM CONSTRUCTION PRINCIPLES IN GENERAL

9 The landmark case of Markman v. Westview Instruments, Inc., 517 U.S. 370 (1996),  
10 made claim construction a question of law for this Court to decide. Since Markman, the Federal  
11 Circuit has progressively refined the claim-construction process and established a detailed  
12 methodology for construing patent claims.

13 In its significant recent opinion in Texas Digital Systems, Inc. v. Telegenix, Inc., 308  
14 F.3d 1193 (Fed. Cir. 2002), the Federal Circuit synthesized the claim construction process and,  
15 in doing so, defined a roadmap for construing patent claims. First, the ordinary meaning of each  
16 disputed term is determined. Id. at 1202, 1204. There is a “heavy presumption” that claim terms  
17 should be interpreted to “have the ordinary meaning that would be attributed to those words by  
18 persons skilled in the relevant art.” Id. at 1202. The Federal Circuit encourages examination of  
19 “relevant dictionaries, encyclopedias and treatises” to determine how those in the art would  
20 understand the claim. Id. at 1205.

21 The Federal Circuit has warned against considering the specification and file history  
22 during this initial step:

23 Consulting the written description and prosecution history as a threshold step in  
24 the claim construction process, before any effort is made to discern the ordinary  
25 and customary meanings attributed to the words themselves, invites a violation of  
our precedent counseling against importing limitations into the claims.

26 Id. at 1204. To avoid this error, the court must first focus on the claim’s ordinary meaning.

27 Second, the patent’s specification and prosecution history are examined for clear  
28 evidence tending to rebut the presumption that a term should be given its ordinary meaning. Id.

1 at 1204 (“In short, the presumption in favor of a dictionary definition will be overcome where  
2 the patentee, acting as his or her own lexicographer, has clearly set forth an explicit definition of  
3 the term different from its ordinary meaning.”). Such evidence may include use of the term in  
4 the specification “in a manner clearly inconsistent with [its] ordinary meaning” and “expressions  
5 of manifest exclusion or restriction” by an inventor that clearly disavow or disclaim scope that  
6 would have otherwise been encompassed by the term. Id.

7 “[U]nless compelled otherwise, a court will give a claim term the full range of its  
8 ordinary meaning as understood by persons skilled in the relevant art.” Id. at 1202. Thus, a  
9 term’s ordinary meaning must be adopted unless clear evidence from the patent’s specification or  
10 prosecution history manifests a departure from the standard usage of the term. Id.

11 The claim’s central role in defining a patentee’s invention is also the basis for one of the  
12 most well-established canons of claim construction: the prohibition against reading features or  
13 limitations into a claim from the patent specification. See, e.g., McCarty v. Lehigh Valley R.R.,  
14 160 U.S. 110, 116 (1895) (“[W]e know of no principle of law which would authorize us to read  
15 into a claim an element which is not present”); Renishaw PLC v. Marposs Societa’ per Azioni,  
16 158 F.3d 1243, 1248 (Fed. Cir. 1998). This rule follows from the separate purposes of the patent  
17 specification and claims. The role of the patent specification is to adequately describe the  
18 invention to enable the public to make and use it once the patent expires. See 35 U.S.C. § 112,  
19 ¶ 1. The role of the claims is completely different. See SRI Int’l v. Matsushita Electric Corp. of  
20 Am., 775 F.2d 1107, 1121 n.14 (Fed. Cir. 1985) (“Specifications teach. Claims claim.”).

21 Patent claims define the inventor’s property right. A patent claim recites a particular  
22 combination of elements that the inventor believes is different than any combination that has  
23 existed before. If it is novel, and is also useful and not obvious, the inventor is entitled to a  
24 patent monopoly for the claimed combination even if it does not include many elements of the  
25 inventor’s preferred embodiment described in the specification. See, e.g., Renishaw, 158 F.3d at  
26 1248 (“[T]he claims define the scope of the right to exclude; the claim construction inquiry,  
27 therefore, begins and ends in all cases with the actual words of the claim....”). It is therefore  
28 both unfair and improper to graft unclaimed elements from the inventor’s specification onto the

1 claims because doing so cheats the patentee of intellectual property to which he or she is entitled  
2 by law. See Texas Digital, 308 F.3d at 1204 ("But if the meaning of words themselves would  
3 not have been understood to persons of skill in the art to be limited only to the examples or  
4 embodiments described in the specification, reading the words in such a confined way would  
5 mandate the wrong result and would violate our proscription of not reading limitations from the  
6 specification into the claims.")(emphasis added).

#### 7 IV. THE LENGTH AND COMPLEXITY OF MICROSOFT'S PROPOSED 8 CONSTRUCTIONS

9 Microsoft's proposed constructions are undoubtedly the longest and most complex claim  
10 constructions ever presented by a patent litigant. Microsoft's definition of VDE alone amounts  
11 to over 2,000 words, including numerous separately defined terms that are incorporated by  
12 reference.<sup>3</sup> That definition is over ten times longer than the longest proposed definition  
13 InterTrust can find in any Federal Circuit opinion. In fact, as best InterTrust can determine,  
14 Microsoft's definition is far longer than any claim construction ever proposed by any party in  
15 any patent litigation.

16 Although VDE is Microsoft's longest definition, it is not alone in its excesses: twelve of  
17 Microsoft's other definitions amount to over one hundred words each. Derwin Decl., ¶ 4. Many  
18 of these include multiple hundreds of words and incorporate other defined terms by reference.

19 InterTrust's patent claims are relatively straightforward. '721 Claim 34, for example,  
20 amounts to a total of 67 words. Microsoft's VDE definition by itself is more than thirty times  
21 longer than the entire claim, not to mention much more complex, yet Microsoft seeks to  
22 incorporate this mammoth definition into the claim despite the fact that the claim itself does not  
23 recite a VDE. If Microsoft's constructions were adopted wholesale, the jury instruction  
24 "explaining" this claim by itself would amount to at least 3,000 words, and probably many more.

25 No jury could possibly understand or apply constructions of this length and complexity.  
26 No jury has ever been asked to do so. Microsoft's proposals are designed to entirely defeat the  
27 purpose of claim construction, since they would render the claims far more difficult to

28 <sup>3</sup> Declaration of Douglas K. Derwin In Support of InterTrust's Claim Construction Position

1 understand, rather than less:

2 [I]n the end, claim construction must result in a phraseology that can be taught to  
3 a jury of lay people. It is not enough simply to construe the claims so that one  
4 skilled in the art will have a definitive meaning. Control Resources, Inc. v. Delta  
5 Electronics, Inc., 133 F. Supp. 2d 121, 127 (D. Mass. 2001); see MacNeill  
6 Engineering Co., Inc. v. Trisport, Ltd., 126 F. Supp. 2d 51, 56 (D. Mass. 2001),  
7 dismissed on appeal; 2001 WL 838410 (Fed. Cir. 2001) ("The Court's 'claim  
8 construction obligation ... involves not only properly construing the claim  
9 language so that the litigants (for the most part skilled in the particular art) will  
10 understand it, but also teaching the chosen construction to the jury in language  
11 that will inform the jury in plain English the legal framework it must apply in  
12 order to do justice.'").

13 SKW Ams. v. Euclid Chem. Co., 231 F. Supp. 2d 626, 639 (N.D. Ohio 2002).

14 Definitions so long and complex as to defy meaningful application are per se  
15 unreasonable.

## 16 V. SPECIFIC CLAIM CONSTRUCTION ISSUES

17 This section sets forth a brief statement of InterTrust's position and supporting evidence,  
18 on each of the specific disputed claim terms.<sup>4</sup> By necessity, these explanations are abbreviated,  
19 and must be read in conjunction with the proposed claim constructions and supporting evidence  
20 contained in the Joint Claim Construction Statement ("JCCS"). Given the number of disputed  
21 terms, and the size and complexity of Microsoft's proposals, it is impossible within the page  
22 limits of this Memorandum for InterTrust to address all (or even a majority) of the specific issues  
23 raised by the Microsoft definitions. Instead, this Memorandum will describe evidence  
24 supporting InterTrust's constructions and will point out one or more significant problems with  
25 each Microsoft definition. For a more general overview, the accompanying Reiter Declaration  
26 includes an explanation of the background of the patents and of the claims as a whole, and may  
27 be consulted by the Court for an understanding of the context in which these claim elements  
28

29 ("Derwin Decl."), ¶ 3.

30 <sup>4</sup> Terms are listed in the order presented in the claims, using the same order as JCCS Exhibit A.  
31 The parties' proposed constructions can be found at the JCCS Exhibit A and Exhibit B locations  
32 cited below in the heading of each section. Evidence citations are to JCCS Exhibit C, unless  
33 otherwise noted. Such citations are given using the tab number from the Exhibit (each tab  
34 corresponding to a particular defined term), and a letter designating the particular quotation (e.g.,  
35 1(A) is a reference to Exhibit C, Tab 1 ("aspect") and in particular to the quotation designated as  
36 "A". References to Exhibit D are to items contained in the list of evidence submitted by  
37 Microsoft in Exhibit D to the JCCS.

1 appear. Reiter Decl., ¶¶ 5-17 and Ex. B.

2 The Court should not assume that InterTrust agrees with sections of Microsoft's proposed  
3 definitions that are not addressed herein. In general, the issues discussed below are exemplary of  
4 the vast majority of limitations improperly incorporated into the Microsoft definitions: those  
5 limitations either contradict the specifications, are completely unsupported, or attempt to  
6 transform preferred embodiments into claim limitations.

7 **A. Global Requirement of a Virtual Distribution Environment (Ex. A, Row 1,  
8 Ex. B, Row 24, Ex. C, Tab 24)**

9 Microsoft asserts that each and every claim requires a Virtual Distribution Environment  
10 ("VDE"), even though this phrase appears in only one of the twelve claims at issue, and even in  
11 that claim the phrase is only in the preamble. Microsoft's definition of Virtual Distribution  
12 Environment includes 690 words, and incorporates separately defined terms that bring the total  
13 to over 2,000 words of text. Microsoft thus asks the Court to read an extraneous 2,000 word  
14 definition into every single claim.

15 In the current section, InterTrust will discuss Microsoft's Global Construction position.  
16 Issues raised by the definition itself are discussed below, in Section Y.

17 **1. The eleven claims other than 900.155<sup>5</sup> do not recite a "Virtual  
18 Distribution Environment" and do not contain any language implying  
19 any such requirement.**

20 None of the eleven claims other than 900.155 includes any mention of a VDE.  
21 Moreover, none of those claims contains any language from which inclusion of a VDE limitation  
22 can be inferred. 193.1, for example, recites a method that can be performed by a single user: a  
23 music file is received, control(s) are used to determine if the music file can be copied to a second  
24 device (e.g., a portable music player); if the control(s) allow the transfer, the music file is  
25 transferred to the second device and the music is played through an audio output at that device.

26 See Reiter Decl., Ex. B, p.1.

27 Compare this claim to Microsoft's definition of VDE. The first numbered paragraph of  
28 that definition is titled "Data Security and Commerce World," and describes a "multi-node world

---

<sup>5</sup> Claim 155 of the '900 patent.

(community)," recites guarantees provided to "all" participants, and expressly excludes "anything less than or different than this." The sixth numbered paragraph specifies that "each VDE node has the innate ability to perform any role identified in the patent application (e.g., end user, content packager, distributor, Clearinghouse, etc.)" The seventh numbered paragraph is titled "Comprehensive Range of Functions" and states that "VDE comprehensively governs (Controls) all security and commerce activities identified in the patent application, including (a) metering, budgeting, monitoring, reporting, and auditing information usage, (b) billing and paying for information usage, and (c) negotiating, signing and enforcing contracts . . . ."

None of these elements has anything to do with the claim at issue. 193.1 does not require a "world," nor a multi-node community, nor guarantees to "all" participants. 193.1 does not mention or require content packagers, distributors or clearinghouses, nor does it have any language requiring or suggesting that "each" VDE node can play any role.

Similar points can be made relating to the other sections of the Microsoft definition. These and many other requirements from Microsoft's 2,000 word definition of VDE are completely irrelevant to 193.1, and equally irrelevant to the other claims at issue in this litigation. For example, 721.1 consists of 67 words, not one of which requires, implies or even relates to the VDE limitations Microsoft seeks to graft onto it. The absurdity of reading 2,000 additional words of limitation into a 67-word claim is obvious.

## **2. Incorporation of Virtual Distribution Environment into Claims Neither Reciting Nor Implying Such a Limitation Is Improper.**

The evidence cited by Microsoft in Exhibit D to the JCCS indicates that Microsoft intends to argue that statements in the '193 and '683 patents regarding the "invention" compel reading all elements of a VDE into all claims. Although statements in an application regarding the "invention" may be taken into account in claim interpretation, neither the Federal Circuit nor any District Court has ever used such statements to read elements such as those proposed by Microsoft into all claims. Instead, the case law is clear that, under circumstances such as those presented in this case, statements in a patent's specification about the "invention" do not serve to limit the scope of issued claims.

1                   a.     **The eleven claims other than 900.155 contain no limitations relating to**  
2                           **a Virtual Distribution Environment.**

3                   According to the Federal Circuit, statements in an application regarding the invention  
4 cannot be read into the claims absent a relevant limitation in the claims themselves. For  
5 example, in Amgen Inc. v. Hoechst Marion Roussel, Inc., 314 F.3d 1313 (Fed. Cir. 2003),  
6 although the patent specification stated that, “the invention [was] ‘uniquely characterized’ by” a  
7 particular element in dispute, the asserted claims made no reference to that element, and the  
8 Federal Circuit held as follows:

9                   The statement that the invention is “uniquely characterized” by the expression of  
10 exogenous DNA sequences does not impel us to accept TKT’s position when the  
11 asserted claims do not contain such an express limitation.

12 314 F.3d at 1326.

13                   The Federal Circuit ruled similarly in Renishaw PLC v. Marposs Societa’ Per Azioni,  
14 158 F.3d 1243 (Fed. Cir. 1998):

15                   [I]t is manifest that a claim must explicitly recite a term in need of definition  
16 before a definition may enter the claim from the written description. . . .

17                   Thus, a party wishing to use statements in the written description to confine or  
18 otherwise affect a patent’s scope must, at the very least, point to a term or terms in  
19 the claim with which to draw in those statements. Without any claim term that is  
20 susceptible of clarification by the written description, there is no legitimate way to  
21 narrow the property right.

22 158 F.3d 1243, 1248.

23                   The eleven claims other than 900.155 do not recite a VDE. Nor do they include any  
24 other limitations that require one. Reiter Decl., ¶¶ 20-23.

25                   b.     **Statements in the specifications do not clearly disclaim patentable**  
26                           **subject matter, and therefore cannot be used to limit the claims.**

27                   The Federal Circuit has repeatedly held that, in order to limit the scope of a claim,  
28 specification statements about the “invention” must clearly and unambiguously exclude or  
disclaim certain embodiments. As noted, in Amgen the patent specification stated that, “the  
invention is ‘uniquely characterized’ by” a particular element. 314 F.3d at 1326. The Federal  
Circuit held, however, that this statement could not limit the claims: “Amgen’s statements  
simply do not clearly indicate that exogenous expression is the only possible mode of the

1 invention or that other methods were outside the stated purpose of the invention.” 314 F.3d at  
2 1334.

3 Likewise, in Honeywell Inc. v. Victor Co. of Japan, Ltd., 298 F.3d 1317 (Fed. Cir. 2002),  
4 the Federal Circuit held that, in order to be given effect as a claim limitation, “invention”  
5 language in the specification must constitute a “broad and unequivocal” disclaimer, such as an  
6 explicit statement in the specification that “all embodiments of the present invention” include a  
7 specific feature. 298 F.3d at 1325. See also Teleflex, Inc. v. Ficosa North America Corp., 299  
8 F.3d 1313,1324 (Fed. Cir. 2002) (requiring “expressions of manifest exclusion or restriction,  
9 representing a clear disavowal of claim scope”); Moore U.S.A., Inc. v. Standard Register Co.,  
10 229 F.3d 1091, 1111 (Fed. Cir. 2000) (references to the “present invention” or “aspects” of the  
11 “present invention” did not constitute claim limitations), cert. denied, 532 U.S. 1008 (2001).

12 The Federal Circuit has also held that specification statements about the importance of  
13 features or the intent to solve certain problems do not govern claim construction in the absence  
14 of express related language in the claims:

15 [T]he fact that the claimed composition was designed to solve certain problems of  
16 the prior art and the fact that the patentee noted the functional import of having a  
17 homogeneous cast does not mean that we must attribute a function to the  
nonfunctional phrase “substantially uniform.” Where the function is not recited in  
the claim itself by the patentee, we do not import such a limitation.

18 Ecolab, Inc. v. Envirochem, Inc., 264 F.3d 1358, 1367 (Fed. Cir. 2001).

19 The InterTrust specifications contain no language even remotely similar to the statement  
20 in Amgen that the invention was “uniquely characterized” by an element, a statement the Federal  
21 Circuit found insufficient to act as a binding limitation on all claims. The specifications contain  
22 no explicit disclaimers of any subject matter, nor are there any unambiguous (or even  
23 ambiguous) statements to the effect that all embodiments other than a complete VDE are outside  
24 the scope of the patents.

25 **c. Specification statements about the “invention” are only one factor in**  
26 **claim interpretation, and must be interpreted in light of the entire**  
**specification and file history.**

27 Specification statements about “the invention” must be read in light of the specification  
28 and file history as a whole, and such statements do not limit the claims if the rest of the



1 specification and file history do not indicate that such a limitation was intended. Rambus Inc. v.  
2 Infineon Techs. Ag, 318 F.3d 1081, 1094-95 (Fed. Cir. 2003).<sup>6</sup>

3 In the present case, there are numerous aspects of the specification and file history that  
4 contradict Microsoft's argument that VDE must be read into all the claims.

5 (i) **The Patent Office ruled that the parent InterTrust patent**  
6 **application involved five separate and independent classes of**  
**invention.**

7 Although Microsoft would have the Court read the patent specifications as if they  
8 described a single "invention," and thereby read that "invention" into every single claim, the file  
9 history conclusively rebuts that argument. Not only did the Patent Office not find that the  
10 InterTrust specification described a single invention, it held that the parent InterTrust patent  
11 application claimed five separate categories of invention. It further held that these categories of  
12 invention each had "separate utility" separate and apart from any overall combination (e.g., a  
13 VDE). September 25, 1996 Office Action, pp. 2-3 (24(BB)). The Patent Office's ruling  
14 included the following text:

15 1. Restriction to one of the following inventions is required under 35 U.S.C. § 121:

16 Group I . . . drawn to a secure component-based operating process, classified in Class  
17 380, subclass 25.

18 Group II . . . drawn to method(s) for managing a resource or operating, classified in  
19 Class 380, subclass 4.

20 Group III . . . drawn to a secure method, classified in Class 380, subclass 3.

21 Group IV . . . drawn to [a] method of negotiating electronic contracts, classified in Class  
22 364, subclass 401.

23 Group V . . . drawn to methods of auditing a resource, classified in Class 364, subclass  
24 406.

25 **The inventions are distinct, each from the other because of the following reasons:**

26 2. Inventions of Groups I-V are related as subcombinations disclosed as usable together  
27 in a single combination. The subcombinations are distinct from each other if they are  
28 shown to be separately usable. In the instant case, invention of Group I has separate  
utility such as protecting executable code from computer viruses. Invention of Group II  
has separate utility such as a computer network administration. Invention of Group III  
has separate utility such as protection of software. Invention of Group IV has separate  
utility such as a contract bidding procedure. Invention of Group V has separate utility  
such as auditing pay television. . . .

<sup>6</sup> InterTrust is providing a courtesy copy of the Rambus opinion as it appears on Westlaw.

1 3. Because these inventions are distinct for the reasons given above and have  
2 acquired a separate status in the art as shown by their different classification,  
3 restriction for examination purposes as indicated is proper.

4 4. Because these inventions are distinct for the reasons given above and have  
5 acquired a separate status in the art because of their recognized divergent subject  
6 matter, restriction for examination purposes as indicated is proper.

7 24(BB) (emphasis added).

8 The Patent Office could hardly have been clearer: InterTrust's parent application  
9 involved five separate classes of invention. Each class of invention had utility separate from all  
10 of the others. Each class of invention was recognized in the art as relating to a divergent subject  
11 matter.

12 Based on this ruling, the Patent Office entered a "restriction" requirement, in which  
13 InterTrust was directed to pick one class of inventions to be pursued in the application.  
14 InterTrust did so, and also filed separate "divisional" applications relating to the other categories  
15 of inventions. Derwin Decl., ¶ 2.

16 Of the patents now at issue, '193, '891 and '912 have specifications identical to the  
17 original application, and correspond to three of the different invention categories identified by  
18 the Patent Office. The '900 is a continuation-in-part and also includes all of the text from the  
19 original application. Derwin Decl., ¶ 2. Thus, of the specification quotations cited by Microsoft  
20 in support of its VDE "global construction" argument virtually all were present in the original  
21 InterTrust application, the application determined by the Patent Office to involve five separate  
22 categories of invention.

23 The Federal Circuit has emphasized that divisional applications, such as those filed in this  
24 case, involve separate and independent inventions:

25 A 'divisional' application, . . . is one carved out of an earlier application which  
26 disclosed and claimed more than one independent invention, the result being that  
27 **the divisional application claims only one or more, but not all, of the**  
28 **independent inventions of the earlier application.**

Transco Prods, Inc. v. Performance Contracting, 38 F.3d 551, 555 (Fed. Cir. 1994) (citing The  
Manual of Patent Examination Procedures, 1988 § 201.06) (emphasis added), cert. denied, 513

1 U.S. 1151 (1995).

2 The Rambus case cited above also involved a restriction requirement issued by the Patent  
3 Office, a factor noted by the Federal Circuit in its holding that statements regarding the  
4 "invention" could not be read into all claims. 318 F.3d at 1095.<sup>7</sup>

5 The Patent Office split the InterTrust patent application into five separate categories of  
6 invention. Microsoft now seeks to reverse that action, asking the Court to interpret the resulting  
7 patents as if they involved a single invention (VDE) and to read that "invention" into every  
8 single patent claim. Microsoft's position is directly contrary to the Patent Office's decision, a  
9 decision to which this Court is required to give,

10 the deference that is due to a qualified government agency presumed to have properly  
11 done its job, which includes one or more examiners who are assumed to have some  
12 expertise in interpreting the references and to be familiar from their work with the level  
13 of skill in the art and whose duty it is to issue only valid patents . . . .

14 McGinley v. Franklin Sports, Inc., 262 F.3d 1339, 1353 (Fed. Cir. 2001).

15 (ii) Microsoft's interpretation of "the invention" is contradicted by  
16 the claims.

17 In Rambus, the Federal Circuit held that specification statements regarding "the  
18 invention" did not limit the claims. One factor it cited was the fact that the patentee had  
19 submitted some claims that expressly recited the element characterized in the specification as  
20 "the invention," thereby making it clear that the specification statements about "the invention"  
21 were not intended as a limitation on the claims in general, since otherwise the express inclusion  
22 of that element in other claims would have been redundant. 318 F.3d at 1095.

23 Exactly the same situation is present here. U.S. Patent No. 5,949,876 is an InterTrust  
24 patent issuing as a direct continuation from the original February 1995 patent application. It  
25 therefore includes the same specification as the '193 patent, including the same statements

26 <sup>7</sup> The Rambus discussion of the restriction requirement is not exactly parallel to the present  
27 facts, since at least one of the restrictions involved in that case apparently involved the exact  
28 claim limitation that was at issue, whereas none of the restrictions involved in the present case  
specifically mentions "Virtual Distribution Environment." It is indisputable, however, that the  
Patent Office in this case determined that multiple classes of invention were presented by the  
InterTrust applications, thereby contradicting any implication that specification references to  
"the invention" mean that all claims must be interpreted in light of a single invention.

1 regarding "the invention" and VDE that Microsoft has cited. The '876 patent includes numerous  
2 dependent claims adding an express requirement that a process or method include a VDE. 24(J).  
3 These dependent claims thus make it clear that claims that do **not** expressly recite a "Virtual  
4 Distribution Environment" were not intended to, and cannot be interpreted to include one.

5 **B. Secure/Security (Ex. A, Row 3, Ex. B, Row 19, Ex. C, Tab 19).**

6 Both parties acknowledge that the terms "secure" and "security" require some degree of  
7 protection against certain threats. InterTrust's proposed definition is consistent with the plain  
8 meaning of these terms as well as the patent specifications. It requires one or more mechanisms  
9 to prevent, detect, or discourage misuse of or interference with information or processes, and  
10 provides examples of the types of mechanisms that may be involved.

11 In contrast, Microsoft burdens these claim terms with numerous additional requirements  
12 that are inconsistent with both the ordinary meaning and the way these terms are used in the  
13 specifications. Two of these unwarranted additional requirements are addressed below.

14 **1. Microsoft's requirement that five specified properties be protected.**

15 Microsoft defines the word "secure" to require, in every instance, protection of five  
16 specified properties (availability, secrecy, integrity, authenticity and nonrepudiation). The  
17 specifications contradict this reading.

18 The specifications frequently use the words "secure" or "security" to refer to the use of  
19 one or more of a collection of protection mechanisms, without requiring the comprehensive  
20 protection of all of the properties specified by Microsoft. The following passage, for example,  
21 could hardly be clearer:

22 In one embodiment, the portable appliance 2600 could support **secure (in this**  
23 **instance encrypted and/or authenticated)** two-way communications with a retail  
24 terminal which may contain a VDE electronic appliance 600 or communicate with a  
retailer's or third party provider's VDE electronic appliance 600.

25 '193 patent 233:25-30 (19(H) (emphasis added).

26 This passage describes "secure" in terms of encryption and/or authentication. These  
27 amount at best to two of the properties from Microsoft's list (secrecy and authenticity). No  
28 mention is made of availability, integrity or nonrepudiation. See also Reiter Decl., ¶ 28,

1 discussing 19(A) ("security" referring to concealment and authentication), 19(B), ("secure"  
2 referring to concealment and authentication), 19(C) ("security" referring to concealment and  
3 tamper resistance), 19(D) ("security" referring to concealment and authentication), 19(E)  
4 ("security" referring to concealment, tamper resistance and access control), 19(F) ("secure"  
5 referring to concealment), 19(G) ("secure" referring to tamper resistance), 19(H) ("secure"  
6 referring to concealment and/or authentication), 19(I) ("secure" referring to concealment).

7 Microsoft's definition requires that all five specified properties be protected. As used in  
8 the specification, however, the term "secure" often means protection of fewer than these five  
9 properties. Microsoft's definition is inconsistent with the specifications and should be rejected.

10 **2. Microsoft's requirement that "all users" be "guaranteed" protection against "all**  
11 **of the identified threats"**

12 Microsoft's definition requires a guarantee to "all users" of absolute protection against all  
13 identified threats. This aspect of Microsoft's definition also contradicts the specifications, which  
14 make it clear that "secure" and "security" do not require absolute protection, but instead require  
15 only that security be sufficient for an intended purpose:

16 The level of security and tamper resistance required for trusted SPU hardware processes  
17 depends on the commercial requirements of particular markets or market niches, **and**  
18 **may vary widely.**

19 193 patent at 49:59-62 (19(J)) (emphasis added). See also 19(B) ("sufficient security  
20 (sufficiently trusted) for the intended commercial purposes"), 19(M), 19(N). The specifications  
21 also describe mechanisms used to limit the effects of a security breach, something that would be  
22 inconceivable if "security" or "secure" required absolute protection. See, e.g., 19(K), 19(L),  
23 19(R), 19(S), 19(T).

24 Moreover, it is understood in the art that security can never be absolute. See, e.g.,  
25 19(BB) ("One hundred percent security cannot be achieved") 19(EE) ("security is a relative, not  
26 an absolute concept"), 19(X), 19(Y), 19(Z), 19(AA), 19(CC), 19(DD).

27 Microsoft's definition requires that absolute security be guaranteed to all participants and  
28 against all threats. This is inconsistent with use of this term in the specification, and with the  
universal understanding in the field, not to mention common sense. No one of ordinary skill in

1 the art would interpret "secure" in this manner. Microsoft's construction is an attempt to define  
2 the term in a manner impossible for any real world system to attain. That construction should be  
3 rejected.

4 **C. Budget (Ex. A, Row 4, Ex. B, Row 3, Ex. C, Tab 3).**

5 In the specifications, "budget" is used consistently with its normal English meaning  
6 (3(A)), and InterTrust's definition of "information specifying a limitation on usage" reflects that  
7 meaning (3(L)). Microsoft similarly defines this term as referring to a "limitation on use," but  
8 then distorts this plain meaning into a budget "method," consisting of instructions and related  
9 data. The specifications, however, explicitly distinguish between a "BUDGET method" and the  
10 word "budget."

11 In the example shown in Figure 41d, a distributor at a VDE distributor node (106) might  
12 request budget from a content creator at another node (102). . . . The creator 102 may  
13 decide to grant budget to the distributor 106 and processes a distribute event (1452 in  
14 BUDGET method 1510 at VDE node 102). A result of processing the distribute event  
15 within the BUDGET method might be a secure communication (1454) between VDE  
16 nodes 102 and 106 by which a budget granting use and redistribute rights to the  
17 distributor 106 may be transferred from the creator 102 to the distributor. The  
18 distributor's VDE node 106 may respond to the receipt of the budget information by  
19 processing the communication using the reply process 1475B of the BUDGET method  
20 1510. The reply event processing 1475B might, for example, install a budget and PERC  
21 808 within the distributor's VDE 106 node to permit the distributor to access content or  
22 processes for which access is control at least in part by the budget and/or PERC.

23 '193 patent, 172:61-173:14 (3(C)) (emphasis added).

24 This passage is unmistakable: the word "budget" does not necessarily mean a "BUDGET  
25 method." A "BUDGET method" is a means to grant a "budget," but it is impossible to read this  
26 passage without understanding that the word "budget," by itself, does not mean "BUDGET  
27 method." See also 3(D) ("BUDGET method 408 may store budget information"), 3(E)  
28 ("BUDGET method" used to process "budget information").

Microsoft's citations from the specification indicating that a "budget" may be a type of  
method are not inconsistent with InterTrust's interpretation, since InterTrust agrees that a budget  
method is one possible embodiment of a budget. But that is all it is: one example of how a  
budget may be specified. Thus, item (1) from Microsoft's Exhibit D support for "budget" refers  
not to the word "budget" in general, but to, "'Budgets' 308 shown in FIG. 5B." The larger

1 context for this passage is shown in 3(F), which makes it clear that the passage cited by  
2 Microsoft relates to one specific example of a budget, i.e., "Budgets 308" from Figure 5B, a  
3 figure that provides additional detail on the "preferred embodiment" shown in FIG. 5A, itself  
4 described as merely an "example." Reading preferred embodiments from the specification into  
5 the claims violates basic Federal Circuit claim construction principles. Laitram Corp. v.  
6 Cambridge Wire Cloth Co., 863 F.2d 855, 865 (Fed. Cir. 1988) ("References to a preferred  
7 embodiment, such as those often present in a specification, are not claim limitations."), cert.  
8 denied, 490 U.S. 1068 (1989).

9 Microsoft's definition also requires that a budget constitute a "decrementable numerical  
10 limitation." There is no basis in the specification (or the normal meaning of "budget") for any  
11 requirement that this constitute a "decrementable" value, as opposed to a value that is  
12 incremented until a limit is reached. Thus, a budget specifying that a user has the right to make  
13 three copies of content could be implemented as a decrementable value (starting with "3" and  
14 counting down each time a copy is made until "0" is reached) or as an incrementable value  
15 (starting with "0" and counting up until the value of 3 is reached). This is an implementation  
16 detail, and both types of value are supported in the specification. See, e.g., 3(H) (describing an  
17 "ascending use counter" and a "descending use counter.") There is no basis for limiting budgets  
18 to a decrementable value. This constitutes yet another Microsoft attempt to read a particular  
19 specification embodiment into the claims, an attempt that is particularly misguided in this case,  
20 since an alternate embodiment (an incrementable counter) is also disclosed.

21 **D. Control (noun) (Ex. A, Row 4, Ex. B, Row 8, Ex. C, Tab 8).**

22 Although the specification contains no explicit definition for "control," it does indicate  
23 that "rules and controls" are equated with "control information." See, e.g., 8(A), 8(B); see also  
24 8(C) ("control" and "control information" used interchangeably).

25 Control information can consist of either programming (e.g., load modules) or data. See,  
26 e.g., 8(D) (load modules, data and methods), 8(F) (a key is control information), 8(G)  
27 (executable programming such as load modules), 8(H) (use of "and/or" making it clear that  
28 control information can consist of methods, or load modules, or mediating data or component

1 assemblies), 8(I) (software and parameter data).

2 In the '193 and related file histories, prior art data items were repeatedly interpreted as  
3 constituting "controls." See, e.g., 8(W) ("control" read onto personal identification information),  
4 8(X) ("control" read onto a list of checkwords), 8(Y) ("control" read onto password), 8(Z)  
5 ("control" read onto security code attribute indicating security levels).

6 Thus, "controls" can consist of various types of information, including programming  
7 (load modules, methods, component assemblies) and data. This is consistent with the InterTrust  
8 construction of the term.

9 The InterTrust construction also specifies that controls can govern operations on, or use  
10 of, resources (e.g., content), including permitted, required or prevented operations, the nature and  
11 extent of operations, and the consequences of operations. Again, this is consistent with use of  
12 the term control information in the specification. See, e.g., 8(J), 8(A), 8(H), 8(K), 8(L), 8(M),  
13 8(B), 8(N), 8(O).

14 Microsoft's definition requires that controls be "executable." Although the parties  
15 disagree regarding the definition of "executable," neither party's proposed definition would  
16 include data. As is established above, however, the patents indicate that "controls" may include  
17 data. Microsoft's incorporation of "executable" into the definition of controls is therefore  
18 improper.

19 The Microsoft definition further requires that controls execute in a Secure Processing  
20 Environment ("SPE"). However, the patents make it clear that an SPE is a particular  
21 embodiment, and clearly disclose an alternate embodiment known as a Host Processing  
22 Environment ("HPE"), an embodiment excluded by the Microsoft definition. See Protected  
23 Processing Environment (§ P, below). The patents explicitly state that any operation that carried  
24 out by an SPE can also be carried out by an HPE. 16(D).

25 Microsoft's definition also requires the ability to modify controls. MS def., ¶ (7). This  
26 is a preferred embodiment, and in any event is a capability provided by the ROS (an operating  
27 system described in the specification) rather than by the controls themselves. 8(Q).

28 Microsoft also seeks to apply the general definition of "control (n.)" to "user controls" as



1 recited in 683.2. InterTrust objects to this, since "user controls" was a term on the parties' initial  
2 list of claim terms to be construed, but was not selected for the initial hearing, and InterTrust  
3 therefore requests that the Court reserve construction of this term.

4       Moreover, "user controls" in claim 683.2 is entirely unrelated to the "controls" discussed  
5 above. That sense of "control" is synonymous with "rules," and is a form of information that  
6 tells the system what the user may and may not do with the relevant content. By contrast, as  
7 used in 683.2, "user controls" refer to the hardware used to control a computer (such as a  
8 keyboard or mouse), rather than information or programming. In the claim, user controls are  
9 listed with other hardware elements (also including communications port, processor and  
10 memory). Significantly the digital information recited in the claim is explicitly identified as  
11 being stored in the memory (first secure container, governed item, first secure container rule,  
12 etc.), whereas "user controls" is listed as an element separate and apart from the memory.  
13 Moreover, in the file history the Examiner used a keyboard as an example of "user controls."  
14 8(AA). Thus, the file history and the claim make it clear that "user controls" means something  
15 entirely different from either party's proposed construction of "control" as used in the other  
16 claims.

17       **E. Copy/Copied/Copying (Ex. A, Row 5, Ex. B, Row 10, Ex. C, Tab 10).**

18       InterTrust's proposed definition is the plain English meaning, based on "reproduce."  
19 This is consistent with the generally understood definition of this term. 10(K), 10(L), 10(M).

20       Microsoft's first sentence is consistent with InterTrust's construction, except for  
21 Microsoft's requirements that "all" of a file be reproduced and that this constitute a "complete  
22 physical block of data." The specification contradicts these requirements, since it explicitly uses  
23 the word "copy" to refer to a partial reproduction. 10(A), 10(B).

24       The definitions also differ in that InterTrust's definition requires that the copy be usable,  
25 whereas Microsoft's allows a copy to be ephemeral, unusable or inaccessible. MS def., ¶ (3).

26       As used in the relevant claims (193.1, 193.11, 193.15, 193.19), the whole point of making  
27 a "copy" is to use it. Microsoft's definition, however, would define the word "copy" to include  
28 reproductions that are ephemeral, unusable and inaccessible, thus interpreting this term to

1 include internal "phantom" reproductions made by the computer in the process of using a file.

2 As Dr. Reiter's Declaration explains, such temporary internal reproductions are  
3 automatically created by the computer for purposes of the computer's internal processing, and  
4 the user is never even aware of their existence. Reiter Decl., ¶¶ 34-40. For example, such  
5 reproductions are made every time a file is opened (e.g., a memo is brought up on a computer's  
6 screen), even though, from the perspective of the user, such actions have nothing whatever to do  
7 with making a copy of the file.

8 Defining such automatically-generated, unusable reproductions as "copies" leads to an  
9 absurd interpretation of the claims. For example, in 193.1, the user receives a budget specifying  
10 the number of "copies" that can be made of a file. If "copy" means internal, phantom  
11 reproductions, a portion of that budget would be used up every time the user made any use of the  
12 file, even if the user did not deliberately make a "copy," and even if the action did not result in  
13 anything the user would recognize as a "copy." Thus, a budget to make three copies of the file  
14 would be used up if the user opened the file three times, even if the user never created any  
15 permanent, usable copies at all. A user whose paid-for budget to make copies of a file was used  
16 up by merely opening the file is a user who would probably be looking for a good consumer-  
17 fraud attorney.

18 Even worse, if Microsoft's interpretation of "copy" is accepted, once the 193.1 budget to  
19 make copies was exhausted, the user would not only lose the ability to make actual copies, but  
20 would also lose any ability to even open the file, since the act of opening the file causes the  
21 creation of internal phantom reproductions. Thus, a user with a budget to make three copies of  
22 the file would be able to open the file three times, after which he or she would have no ability to  
23 make any other use of the file whatever.

24 Such an interpretation is absurd. 193.1 clearly contemplates the user receiving a budget  
25 to make deliberately-intended copies that the user (or someone else) can make use of.  
26 Interpreting "copy" so that the copy budget would be used up by internal phantom reproductions  
27 requires completely ignoring the context of the claim. See Reiter Decl., ¶¶ 34-40 and § F,  
28 immediately below.

1           **F.     Budget Specifying the Number of Copies Which Can Be Made of Said Digital**  
2           **File (Ex. A, Row 6, Ex. B, Row 25, Ex. C, Tab 25).**

3           This claim phrase is straightforward. It incorporates two separately defined terms  
4 (Budget and Copies), but there is no reason to interpret it using anything other than its plain  
5 English meaning.

6           Microsoft's definition, on the other hand, incorporates requirements that are unsupported  
7 by the phrase and contradict the specifications.

8           (1) Microsoft requires that the budget state "the total number of copies (whether or not  
9 decrypted, long-lived, or accessible)." No such requirement is imposed by the claim term and, as  
10 is described above (see § E), this requirement makes no sense, since the budget would be  
11 exhausted by internal, "phantom" reproductions of no benefit to the user. See Reiter Decl.,  
12 ¶¶ 34-40.

13           (2) The Microsoft construction also requires that "No process, user, or device is able to  
14 make another copy of the Digital File once this number of copies has been made." The  
15 specification, however, explicitly describes processes that can be used to "refresh" budgets, so  
16 that a budget that has been exhausted (e.g., reached zero) can be increased. See, e.g., 25(O)  
17 (describing the acquisition of "additional budgets if the user wishes to continue to use the  
18 traveling object after the exhaustion of the available budget(s)"), 25(P) ("Once the distributor  
19 106 has used some or all of her budget, she may desire to obtain additional budget") 25(Q)  
20 ("clearinghouse may handle the end user's request for additional budget"). Microsoft's proposed  
21 addition of this limitation is thus directly contradicted by the specification.

22           **G.     Control (verb) (Ex. A, Row 7, Ex. B, Row 9, Ex. C, Tab 9).**

23           "Control," used as a verb (e.g., "controlling") is not specially defined in the  
24 specifications. The InterTrust construction is based on the common English definition for the  
25 term (9(O)), a construction supported by the use of this term in the specification. Passages cited  
26 in Ex. C at 9(A), 9(B), 9(C), 9(D), 9(E) and 9(F), for example, use the verb form of "control" to  
27 refer to conventional hardware or software operations, that cause or prevent certain acts or  
28 events. Reiter Decl., ¶ 42.

1 Microsoft proposes a lengthy and highly complicated definition for this term, without any  
2 support whatsoever. The evidence cited by Microsoft contains no indication that the verb form  
3 of control is defined in any particular manner in the specification, and certainly does not support  
4 the lengthy and complex definition proposed by Microsoft. In fact, the majority of Microsoft's  
5 Exhibit D evidence for this term (Ex. D, Row 9) relates to the noun form of "control," and does  
6 not even mention the verb form.

7 Not only is the Microsoft definition unsupported by the specification, restrictions  
8 contained in that definition are actually contradicted by the specification. For example,  
9 Microsoft requires that a controlled action cannot otherwise be taken by any user, process or  
10 device. This restriction ignores the specification's discussion of alternate control structures,  
11 whereby an action not allowed by one control structure may be allowed by another. See 9(G),  
12 9(H), 9(I), 9(J).

13 The Microsoft definition also requires the use of a VDE Secure Processing Environment.  
14 This ignores the specification's discussion of Host Processing Environments, identified as an  
15 alternative to the Secure Processing Environment embodiment. See Protected Processing  
16 Environment (§ P, below); see also 16(D) (HPE can carry out any operation carried out by an  
17 SPE).

18 **H. Controlling the Copies Made of Said Digital File (Ex. A, Row 7, Ex. B, Row**  
19 **26, Ex. C, Tab 26).**

20 The relevant claim (193.1) itself further explains this element as follows: "if said copy  
21 control allows at least a portion of said digital file to be copied and stored on a second device."  
22 This further description, along with the separately defined incorporated terms, fully defines this  
23 element by making it clear that the copy control is used to determine whether a digital file may  
24 be copied to a second device. InterTrust's proposed construction is based on this  
25 straightforward, plain English interpretation.

26 Microsoft requires that the copy control operate within a VDE Secure Processing  
27 Environment. No such requirement is imposed by the claim, and the specification describes  
28 embodiments based on a Host Processing Environment, rather than a Secure Processing

1 Environment. See Protected Processing Environment, § P, below; see also 16(D).

2 The Microsoft definition requires that the copy control control “all copies of the *Digital*  
3 *File*.” The claim contains no such requirement, but instead requires control over copies that are  
4 made, as opposed to all copies that exist. Microsoft’s interpretation apparently would require  
5 that the copy control, operational at the first device, somehow control copies of the file at the  
6 source from which the first device received the file, including copies at other locations to which  
7 that source sent the file. In context, it is clear that the copy control need only govern copies  
8 made by the first device, not all copies that exist.

9 Microsoft further requires that all uses and accesses be prohibited except to the extent  
10 allowed by the copy control(s). This assertion has no support in the claim, and ignores the  
11 possibility that the item may also be governed by an alternate control structure. 26(A), 26(B),  
12 26(C), 26(D).

13 **I. Authentication (Ex. A, Row 27, Ex. B, Row 2, Ex. C, Tab 2).**

14 This word is not specially defined in the specifications or the file histories. Both parties’  
15 proposed definitions focus on identifying something or someone.

16 The specification uses the term “authentication” to refer to various types of identification,  
17 including passwords (2(A), 2(B)), voice prints or retinal scans (2(B)) or certificates attesting that  
18 a device or key can be trusted. 2(C). InterTrust’s proposed construction is consistent with these  
19 specification embodiments.

20 Microsoft’s definition requires establishing that assertions about data integrity (i.e., that  
21 the data have not been altered) and origin integrity (i.e., confirming the source and time of  
22 origination) are genuine. In 193.15, however (the only relevant claim including this term), the  
23 word is used to describe a step involving an identifier associated with a device and/or user.  
24 Requiring “data integrity” and “origin integrity” makes no sense in the context of a user, and  
25 scarcely more sense in the context of a device. Moreover, none of the specification uses of this  
26 term implies such requirements.

27 The Microsoft definition is ambiguous regarding whether authentication requires  
28 uniquely identifying the person or thing authenticated. InterTrust’s proposed definition, on the

1 other hand, allows authentication to identify something or someone either as an individual or as a  
2 member of a group. This is supported by the specification, which describes an "Authenticate  
3 User" process that lets the caller authenticate a specific user ID or a group membership. 2(D).

4 **J. Identifier (Ex. A, Row 28, Ex. B, Row 17, Ex. C, Tab 17).**

5 The InterTrust definition is straightforward and consistent with the normal meaning of  
6 this term and with its use in the specification. See, e.g., 17(A), 17(B).

7 The primary distinction between the parties' definitions concerns whether the identifier  
8 must be unique to an "individual instance" of a person or thing, or whether the identifier can  
9 specify that a person or thing is a member of a group.

10 In 912.8, this term is used in the following context:

11 said load module including executable programming and a header;

12 said header including an execution space **identifier** identifying at  
13 least one aspect of an execution space required for use and/or  
execution of the load module associated with said header;

14 said execution space **identifier** provides the capability for  
15 distinguishing between execution spaces providing a higher  
level of security and execution spaces providing a lower  
16 level of security;

17 A specification embodiment corresponding to this element is described in 30(A), in  
18 which a load module header is described as containing an "execution space code" that  
19 distinguishes SPEs from HPEs, with the explanation that some load modules are required to run  
20 in one type of environment as opposed to the other. This embodiment describes identifying an  
21 execution space as a member of a group (SPE or HPE) and therefore contradicts Microsoft's  
22 interpretation of "identifier" as requiring unique identification. Reiter Decl, ¶¶ 92-94.

23 Similarly, the specification uses the related terms "identification" and "ID" to refer to  
24 identification of an individual or a group. 17(D), 17(E). Thus, interpreting "identifier" as  
25 requiring a unique identification (as opposed to identification as a member of a group) would  
26 contradict the specification.

27 Microsoft also requires that an identifier constitute a "text string." No such requirement  
28 exists in the specification or any relevant claim. An identifier could constitute a string of

1 numbers or bits (e.g., the retail terminal identifier described in 17(B), which might reasonably be  
2 expected to consist of numbers).

3 **K. Clearinghouse (Ex. A, Row 40, Ex. B, Row 4, Ex. C, Tab 4).**

4 The specification describes various embodiments of "clearinghouses," including entities  
5 that provide both financial and administrative services and may collect and distribute  
6 information. See 4(A), 4(B), 4(C), 4(D), 4(E), 4(F), 4(G), describing financial clearinghouses,  
7 document tracking clearinghouses, rights distribution clearinghouses, etc. InterTrust's proposed  
8 construction is straightforward, and describes these various embodiments.

9 Microsoft's construction, on the other hand, requires interpreting "clearinghouses" as  
10 limited to providing "store and forward" services. The specification, however, does not support  
11 limiting "clearinghouse" to this particular embodiment. Thus, Microsoft's Exhibit D quotations  
12 for this term describe other types of clearinghouses (e.g., financial clearinghouses) and none  
13 implies that a clearinghouse must provide "store and forward" services.

14 Nor do Microsoft's excerpts support any requirement that a clearinghouse operate under  
15 the constraints of "VDE security." The specification describes both Visa and AT&T as  
16 "clearinghouses." 4(B), 4(K). These are well-known organizations, and there is no suggestion in  
17 the specification that these organizations use "VDE security," nor would one of ordinary skill in  
18 the art so interpret these references. Reiter Decl., ¶ 48.

19 **L. Use (Ex. A, Row 42, Ex. B, Row 23, Ex. C, Tab 23).**

20 "Use" is a common English word, not specially defined in the specification and not a  
21 term of art. Reiter Decl., ¶ 49. InterTrust proposes giving the term its normal English meaning.  
22 See, e.g., 23(A).

23 Microsoft's proposed definition, by contrast, requires that "use" is allowed only through  
24 execution of controls. This is incorrect, since (a) controls include non-executable data (see  
25 Control, § D, above) and (b) the word "use" is a plain English word, with no technical meaning,  
26 and does not require or imply the use of any controls.

27 Notably, in the claims, when the "use" of an item is required to be governed by controls,  
28 this is explicitly set forth as a claim limitation:

1 683.2: securely applying, at said first appliance through use of said at least one  
2 resource said first entity's control and said second entity's control to govern use of  
said data item

3 Such claim limitations would be superfluous if the word "use" itself required the  
4 application of controls.

5 **M. Secure Container (Ex. A, Row 57, Ex. B, Row 20, Ex. C, Tab 20).**

6 The term "container" is not explicitly defined in the specification. The specification  
7 does, however, give numerous examples of containers that are consistent with InterTrust's  
8 proposed definition. 20(A). In addition, InterTrust's definition closely tracks the accepted  
9 definition of the term "container" in the computer field as of the relevant filing date. 20(J),  
10 20(K). Note that such "containers" represent digital file formats, rather than physical containers.

11 The specification also contains no explicit definition of "secure container." InterTrust's  
12 definition of a Secure Container as a container that is "Secure" is simple, plain English, and is  
13 supported by the specification. 20(B), 20(C).

14 Microsoft's definition consists of approximately 290 words, including nine separately  
15 defined terms, many of which incorporate their own separately defined terms. Derwin Decl., ¶ 4.  
16 Such a definition is so long and complex as to render it impossible for the jury to understand or  
17 apply it.

18 Microsoft's definition also suffers from a number of specific defects, including the  
19 following:

20 (1) Microsoft requires that a secure container "cryptographically protects" information.  
21 MS def., ¶ (1). Although the meaning of this statement is not entirely clear, it appears to require  
22 encrypting the secure container. The specification makes it clear that secure containers need not  
23 be encrypted (they can be "otherwise secured") and that protection need only be partial. 20(B).

24 (2) Microsoft requires that a secure container "encapsulates" its contents. MS def., ¶ 1.  
25 This term is separately defined (in Microsoft's definition of Protected Processing Environment)  
26 as follows: "'Encapsulated' means hidden within an object so that it is not directly accessible  
27 but rather is accessible only through the object's restrictive interface."

28 The specification is clear, however, that the contents of a secure container are not



1 necessarily "hidden within" the secure container but can be located externally, as long as the  
2 container contains a reference to the contents. 20(D), 20(E). Thus, a requirement that a secure  
3 container "encapsulate" its contents is inconsistent with embodiments disclosed in the  
4 specification.

5 (3) The last sentence of the Microsoft definition reads as follows:

6 All VDE-protected information (including protected content, information about  
7 content usage, content-control information, **Controls**, and *Load Modules*) is  
8 encapsulated within a **Secure Container** whenever stored outside a *Secure  
Processing Environment* or secure database.

9 This statement is inaccurate (20(F)), but, in any event, it cannot constitute part of the  
10 definition of a "secure container," since it is not an attribute of a secure container and cannot be  
11 used by a trier of fact to determine whether a particular data structure does or does not constitute  
12 a "secure container." Instead, this passage describes the manner in which certain types of data  
13 are allegedly handled, rather than the properties of the secure containers themselves.

14 (4) Microsoft's definition requires that secure containers can only be opened in Secure  
15 Processing Environments. MS def., ¶ (2). This ignores the specifications' disclosure of the  
16 alternate Host Processing Environment embodiment. See Protected Processing Environment, §  
17 P, below; see also 16(D).

18 (5) Microsoft requires that a secure container can only be opened through decryption of  
19 an encrypted header. MS def., ¶ (2). The encrypted header, however, is described as a preferred  
20 embodiment, and therefore does not constitute a claim limitation. 20(G).

21 (6) Microsoft specifies that a container is not a secure container merely because it is  
22 encrypted and signed. MS def., ¶ (5). The specification provides no support for such a  
23 statement, nor for any requirement that secure containers in fact be encrypted and signed. See,  
24 e.g., 20(B) ("encrypted or otherwise secured.")

25 N. **Contain/Containing** (Ex. A, Row 58, Ex. B, Row 7, Ex. C, Tab 7).

26 InterTrust's definition is based on the plain English meaning of this term. 7(C). This  
27 meaning is consistent with use of the term in the specification. See, e.g., 7(A).

28 The parties' definitions differ primarily in that InterTrust allows "contain" to include

1 storing a reference or pointer indicating where an element may be found, whereas Microsoft  
2 excludes this. InterTrust's position is explicitly supported by the specification:

3 . . . container 302 may "contain" items without those items actually being stored  
4 within the container. For example, the container 302 may reference items that are  
available elsewhere such as in other containers at remote sites . . . .

5 7(B).

6 This passage, and established use in the field directly contradict Microsoft's definition of  
7 "contain" as excluding "addressing." 7(B); Reiter Decl., ¶¶ 51-59.

8 **O. Aspect (Ex. A, Row 60, Ex. B, Row 1, Ex. C, Tab 1).**

9 "Aspect" is not a technical term of art, and is not defined in either the specifications or  
10 the file histories. The term is used in its plain English sense throughout the relevant  
11 specifications. See, e.g., 1(A), 1(B), 1(C), 1(D), 1(E), 1(F), 1(G). InterTrust's proposed  
12 definition is consistent with these uses, and with the word's normal meaning.

13 Microsoft's proposed construction is limited to aspects of an "environment." This is  
14 inconsistent with the use of the term in 912.8 (aspect of an execution space), 861.58 (aspect of  
15 access to or use of secure container contents) and 683.2 (aspect of access to or use of a governed  
16 item). A construction inconsistent with the manner in which the term is used in the claims is  
17 obviously improper.

18 The Microsoft definition also requires a "persistent" element or property. The word  
19 "aspect" does not require or imply persistence. In one relevant specification, the word is used to  
20 refer to a feature that can be destroyed. 1(B). An "aspect" that can be destroyed is obviously an  
21 "aspect" that is not necessarily persistent.

22 **P. Protected Processing Environment (Ex. A, Row 62, Ex. B, Row 18, Ex. C,**  
23 **Tab 18).**

24 The InterTrust definition is closely tied to the description given for Protected Processing  
25 Environments ("PPEs") in the specifications (18(B), 18(C), 18(D)), as well as the manner in  
26 which PPEs are described in claims 721.34 and 683.2, each of which explicitly describes what is  
27 meant by the term.

28 The specifications describe two embodiments of PPE: a Secure Processing Environment

1 (“SPE”), using a special-purpose microprocessor with hardware-based security (a “Secure  
2 Processing Unit”) and a Host Processing Environment (“HPE”), using software-based security  
3 instead of a Secure Processing Unit. 18(B), 18(D), 18(E). InterTrust’s proposed construction  
4 covers both embodiments, as is proper, since the specification explicitly states that any action  
5 that can be taken by an SPE can also be taken by an HPE, albeit possibly with a lower level of  
6 security. 16(D). A number of Microsoft’s definitions, however, would improperly exclude the  
7 HPE embodiment (see, e.g., §§ F, G, H, M, X, Y, DD, above and below).

8 Microsoft’s definition of PPE is considerably longer than the Gettysburg Address. It  
9 contains approximately 345 words in six numbered sections, as well as eleven separately defined  
10 incorporated terms, adding hundreds of additional words. No jury could possibly apply such a  
11 definition in any meaningful way.

12 Given the massive number of limitations Microsoft imposes on this term, a  
13 comprehensive rebuttal would require many pages. Several points, however, are worth noting:

14 (1) Microsoft states that “most” PPEs are Secure Processing Environments incorporating  
15 a Secure Processing Unit. MS deft., ¶ (2). Microsoft does not explain what the other PPEs are,  
16 though the Microsoft definition implies that they fall within the following description: “[a]  
17 facility employing physical facility and user-identity **Authentication** security procedures trusted  
18 by all **VDE** nodes, and the **VDE** node does not Access or Use VDE-protected information, or  
19 assign VDE control information.” MS deft., ¶ (5).

20 As is described above, PPEs incorporating software-based security are known as Host  
21 Processing Environments (“HPEs”), and the specification states that HPEs can perform any  
22 function performed by an SPE. 16(D). Microsoft’s apparent argument that HPEs are used only  
23 in clearinghouses and other physically secure facilities is contradicted by the specifications,  
24 which describe the use of HPEs for end users (18(H)) and in other contexts not involving  
25 clearinghouses. 18(I), 18(K).

26 (2) Microsoft requires that a PPE protects “all information identified in the patent  
27 application as being protected.” To the extent that this requirement is not entirely circular (i.e.,  
28 PPEs protect the information that is protected by PPEs), it appears to imply that all information

1 described in the patents as being protected by any mechanism must also be protected by PPEs.

2 The specifications contain no support for any such requirement.

3 (3) The Microsoft definition states that certain PPEs may "be formed by a general-  
4 purpose CPU that executes all VDE 'security' processes in protected (privileged) mode." MS  
5 def., ¶ (5). No support exists for the protected (privileged) mode restriction. See Host  
6 Processing Environment (§ Z, below).

7 **Q. Digital Signature/Digitally Signing (Ex. A, Row 66, Ex. B, Row 14, Ex. C,  
8 Tab 14).**

9 Although "digital signature" is not defined in the specification, this is a term of art widely  
10 used in the computer security field to refer to information that can be used to determine the  
11 source and/or integrity of a digital file. Reiter Decl., ¶ 62; 14(G). The term "digital signature" is  
12 used in the specification in a manner consistent with the InterTrust construction. 14(A), 14(B).

13 Microsoft's definition requires that a digital signature be "computationally unforgeable."  
14 Neither the specification nor any evidence cited by Microsoft requires any such absolute degree  
15 of protection.<sup>8</sup>

16 **R. Designating (Ex. A, Row 66, Ex. B, Row 12, Ex. C, Tab 12).**

17 This term is not specially defined in the specifications or file histories. InterTrust's  
18 proposed construction is based on the normal English meaning (12(F)), and in the specification  
19 the term is used in accordance with its normal English meaning. 12(A), 12(B), 12(C), 12(D),  
20 12(E).

21 Microsoft requires that designating involve "restricting" something to a particular use.  
22 Neither the English meaning of this term nor the specification supports this limitation. To the  
23 extent that restricting to a particular use is required, this is an aspect of the overall claim in which  
24 this term is used (721.1), and is not inherent in the word "designate." Microsoft has identified no  
25 evidence in support of its construction. None exists.

26 <sup>8</sup> Microsoft's definition of "digital signature" includes a separate definition for the term "key."  
27 The parties dispute the correct definition of "key." This dispute is not relevant to "digital  
28 signature," and therefore is not discussed herein. The meaning of "key" is, however, important  
in other contexts, and InterTrust respectfully requests that the Court refrain from explicitly  
defining "key" at this time, as it is not one of the 30 terms selected for construction.

1           **S.     Device Class (Ex. A, Row 66, Ex. B, Row 13, Ex. C, Tab 13).**

2           This term was explicitly defined in the file history, using the same definition InterTrust  
3 now proposes. 13(A). Such a file history definition is binding. Vitronics Corp. v. Conceptronic,  
4 Inc., 90 F.3d 1576, 1582 (Fed. Cir. 1996) (“Although words in a claim are generally given their  
5 ordinary and customary meaning, a patentee may choose to be his own lexicographer and use  
6 terms in a manner other than their ordinary meaning, as long as the special definition of the term  
7 is clearly stated in the patent specification or file history.”)

8           Microsoft cites no support from the specification for its proposed construction of this  
9 term. That construction is apparently based entirely on the manner in which this term is used  
10 internally at IBM, with no support for applying that construction to the InterTrust patent claims.

11           **T.     Tamper Resistance (Ex. A, Row 67, Ex. B, Row 21, Ex. C, Tab 21).**

12           “Tamper resistance” is not explicitly defined in the specifications. The definition of this  
13 term, however, should follow from the stipulated definition of “Tampering” (JCCS Ex. I), as  
14 InterTrust’s definition does. InterTrust’s construction is also consistent with the use of this term  
15 in the specifications and in relevant extrinsic evidence. 21(A), 21(B), 21(C), 21(D), 21(E).

16           Microsoft states that “tamper resistance” requires a “tamper resistant barrier.” Although  
17 721.34 recites a “tamper resistant barrier,” other claims reciting tamper resistance do not. For  
18 example, 900.155 specifies “tamper-resistant software” with no requirement of a barrier.

19           Microsoft requires that access, observation and interference be prevented. The term is  
20 not, however, tamper **prevention**, but tamper **resistance**, thereby clearly implying that some  
21 degree of resistance less than prevention would be sufficient.

22           Microsoft also requires that all access, observation and interference be prevented.  
23 Tamper resistance should be defined as resistance to Tampering, a separately defined term. By  
24 failing to incorporate this separately defined term, Microsoft requires that Tamper Resistance  
25 protect against actions that do not constitute Tampering (e.g., the definition of Tampering does  
26 not include any reference to “access.”)<sup>9</sup>

27 \_\_\_\_\_  
28 <sup>9</sup> Microsoft repeats the definition of “tampering” in its construction of Tamper Resistance, but  
inexplicably fails to use that definition in defining Tamper Resistance.

1 U. Digitally signing a second load module with a second digital signature  
2 different from the first digital signature, the second digital signature  
3 designating the second load module for use by a second device class having at  
4 least one of tamper resistance and security level different from the at least  
5 one of tamper resistance and security level of the first device class (Ex. A,  
6 Row 67, Ex. B, Row 27, Ex. C, Tab 27).

7 InterTrust's proposed construction is a straightforward explanation of the phrase,  
8 consistent with the embodiment disclosed in the specification. 27(A), 27(B), 27(C), 27(D),  
9 27(E), 27(F), 27(G). Microsoft's definition, on the other hand, builds in a variety of restrictions  
10 that are unsupported by the specification:

11 (1) Microsoft's definition requires that the digital signature be used "as the signature  
12 Key." As described at Reiter Decl., ¶¶ 63-64, a key may be used in a process that creates a  
13 digital signature, but the key and the signature are different things, one used in the process, the  
14 other the result of the process. Dr. Reiter has never heard of a digital signature used as a key to  
15 create a signature, and one of skill in the art would not interpret this phrase to imply any such  
16 requirement. Reiter Decl., ¶¶ 65-66. Neither the claim nor the specification, nor any evidence  
17 proffered by Microsoft supports such a bizarre reading of the phrase.

18 (2) Microsoft's definition also requires that "No VDE device can perform any execution  
19 of any *Load Module* without such authorization." The claim includes no such requirement, and  
20 this is irrelevant to interpretation of this element, since the claim simply requires that two  
21 particular load modules be digitally signed, and does not discuss signing of load modules in  
22 general.

23 (3) Neither this claim phrase nor the entire claim nor the specification as a whole require  
24 or support reading the concept of "VDE device" into this claim, as Microsoft's definition would  
25 require.

26 (4) Microsoft requires that the tamper resistance and security levels be persistent.  
27 Neither the claim nor the specification supports any such requirement.

28 V. **Tamper Resistant Barrier** (Ex. A, Row 71, Ex. B, Row 22, Ex. C, Tab 22).

The term "Tamper Resistant Barrier" should be defined in terms of Tamper Resistance.  
InterTrust's definition does so, and is consistent with use of the term in the specification (e.g.,

1 22(C)). InterTrust's definition makes it clear that such a barrier may consist of hardware or  
2 software, as is required by use of the term in the specification. 22(B).

3 The Microsoft definition requires that a Tamper Resistant Barrier be an "active device."  
4 This is not supported in the specification, and "device" implies hardware, though the  
5 specification states that a tamper-resistant barrier can consist of software. 22(B).

6 Much of Microsoft's definition appears to be taken more or less verbatim from a  
7 description of hardware-based tamper resistant security barrier 502, as described in the  
8 specification. 22(A). This ignores software tamper resistant barriers, which are also described in  
9 the specification, but without the requirements imposed by hardware barriers (e.g., software  
10 tamper resistant barriers are less secure than hardware barriers). 22(B). Microsoft's definition  
11 therefore improperly limits the claims to one particular disclosed embodiment and entirely  
12 ignores a different disclosed embodiment.

13 **W. Executable Programming/Executable (Ex. A, Row 73, Ex. B, Row 15, Ex. C,**  
14 **Tab 15).**

15 Microsoft requires that an "executable" consist exclusively of machine code instructions.  
16 InterTrust's definition would include machine code versions of programs, but also includes  
17 programs written in higher-level languages that require "interpretation," which means the  
18 translation of a program into lower-level machine code instructions. Reiter Decl., ¶¶ 68-70.

19 The specification is clear that "executable" can refer to either lower-level machine code  
20 instructions or higher level instructions that have to be interpreted. See 15(A) (preferred  
21 embodiment is "native" instruction set (i.e., machine code), but an "interpreted" solution (i.e.,  
22 higher level language) may also be used). Reiter Decl. ¶¶ 72-75. See also 15(B), which uses  
23 "executable" to refer to programs written in languages such as Java, a higher-level language  
24 requiring interpretation before being run. Java programs do not constitute machine code. Reiter  
25 Decl., ¶ 71.

26 InterTrust's definition is also consistent with the definition from the Microsoft Computer  
27 Dictionary. 15(C); Reiter Decl., ¶¶ 76-78.

28 Microsoft requires a "complete series of definitions and instructions," thereby implying

1 an entire computer program. Although computer programs are made up of programming, the  
2 term "programming" by itself can mean an entire computer program or merely a portion. Reiter  
3 Decl., ¶ 79.

4 X. Securely applying, at said first appliance through use of said at least one  
5 resource said first entity's control and said second entity's control to govern  
6 use of said data item (Ex. A, Row 85, Ex. B, Row 28, Ex. C, Tab 28).

6 The term "securely applying" is not specially defined in the specification and is not a  
7 term of art. In the specification, the terms "securely applying" and "applying" refer to the  
8 application of control information to govern content. 28(A), 28(B), 28(C), 28(D), 28(E). This is  
9 consistent with InterTrust's proposed construction.

10 (1) The Microsoft definition requires use of a Secure Processing Unit. This ignores the  
11 alternate-embodiment HPE, which does not involve use of a Secure Processing Unit. See  
12 Protected Processing Environment, § P. Moreover, the claim itself recites a "secure operating  
13 environment," and the specification states that a secure operating environment can be either an  
14 SPE or an HPE. 28(H). Thus, requiring that this element take place using a Secure Processing  
15 Unit contradicts the proper interpretation of the claim, which the secure operating environment  
16 recited in the claim can consist of either an SPE or an HPE.

17 In addition, the specification uses "securely" to refer to operations taking place in either  
18 an SPE or an HPE. 28(F). Thus, this word does not imply any requirement of a Secure  
19 Processing Unit.

20 (2) Microsoft's definition of "securely applying" requires executing controls. Controls,  
21 however, include non-executable data (see Control, § D, above), and the specification uses the  
22 term "apply" to relate to applying data (non-executable). 28(G).

23 (3) Microsoft's definition requires that the resource constitute a component part of the  
24 appliance's secure operating environment. The claim imposes no such requirement, and there is  
25 no support for this requirement in the specification or anywhere else.

26 (4) The Microsoft definition requires that this action "governs all use of the data item by  
27 all users, processes, and devices." This limitation is not required by the claim and does not take  
28 into account embodiments describing alternative control structures, in which a use not allowed



1 by one control structure (e.g., a control) might be allowed by a different control structure. See  
2 Control, § D, above.

3 Y. Virtual Distribution Environment (Ex. A, Row 86, Ex. B, Row 24, Ex. C,  
4 Tab 24).

5 Microsoft's Global Construction argument is discussed above. This section will discuss  
6 Virtual Distribution Environment as the term is used in 900.155, the only claim at issue that  
7 actually includes this phrase.

8 "Virtual Distribution Environment" is used only in the preamble of the claim. The  
9 individual elements of 900.155 fully define the recited apparatus, and reference to the preamble  
10 is not necessary to define and understand the claimed apparatus. Reiter Decl. ¶ 80. Under such  
11 circumstances, the preamble does not "give life, meaning and vitality" to the claim and is  
12 irrelevant to claim interpretation. Altiris, Inc. v. Symantec Corp., 318 F.3d 1363, 1371 (Fed. Cir.  
13 2003),<sup>10</sup> Alfred J. Schumer v. Laboratory Computer Systems, Inc., 308 F.3d 1304, 1310 (Fed.  
14 Cir. 2002).

15 Assuming, arguendo, that this phrase needs construction, InterTrust's definition is taken  
16 directly from embodiments of virtual distribution environments described in the specification.  
17 24(A), 24(B), 24(C). Microsoft's definition, on the other hand, is so long and complex as to defy  
18 thorough analysis, at least in the context of the page limits applied to this brief. Nevertheless,  
19 certain broad points can be made.

20 (1) Asking a jury to attempt to comprehend 900.155 by applying a 2,000 word definition  
21 would be asking the impossible. A definition of this length and complexity cannot clarify  
22 interpretation of the claim, but can only lead to confusion.

23 (2) Microsoft's definition requires an SPE. The specification clearly describes use of an  
24 alternate embodiment HPE. See Protected Processing Environment, § P, above.

25 (3) Microsoft's definition incorporates features that would necessarily be "universe-  
26 wide," and could not apply to any particular computer or group of computers, nor to any process  
27 performed on any particular computer or group of computers. Microsoft makes no attempt to

28 <sup>10</sup> InterTrust is providing a courtesy copy of the Altiris opinion as it appears on Westlaw.

1 explain how this “universe-wide” feature of VDE could be applied to a claim relating to a single  
2 device or process. For example, would determining whether a single device infringes a claim  
3 (e.g., whether a particular computer infringes 900.155) require analysis of the entire “universe”  
4 of devices? Such an analysis is obviously impossible and would render this and other claims a  
5 nullity.

6 (4) Microsoft’s definition requires that a VDE “guarantees” various types of security,  
7 and that a VDE is “non-circumventable.” Guaranteed security is impossible in the real world,  
8 and is not required by the specification. See 24(K) through 24(N), 24(P) through 24(AA).

9 **Z. Host Processing Environment (Ex. A, Row 87, Ex. B, Row 16, Ex. C, Tab 16).**

10 The two parties are in agreement that a Host Processing Environment (“HPE”) is distinct  
11 from a Secure Processing Environment (“SPE”), and that an HPE may include software running  
12 on a general-purpose microprocessor.

13 Microsoft is correct that HPEs may be either “secure” or “non-secure.” InterTrust’s  
14 proposed definition is more accurately a definition of secure HPE, but not of a non-secure HPE.  
15 If need be, InterTrust’s definition can be qualified to make it clear that an HPE may be either  
16 secure or non-secure, with the present definition applying to the secure version, and the non-  
17 secure version described as “a processing environment with insufficient security to constitute a  
18 secure HPE.” Such a definition is consistent with use of this term in the specification. 16(A),  
19 16(B), 16(C), 16(D), 16(E).

20 Microsoft’s definition, however, incorporates numerous additional restrictions that are  
21 either unsupported by or contradicted by the specification.

22 (1) Microsoft implies that a HPE consists only of executable programming. This  
23 contradicts 900.155, which identifies various hardware elements as part of the HPE (e.g., a  
24 central processing unit, memory, etc.). This also contradicts Microsoft’s construction of the  
25 claim phrase in which host processing environment appears (“Derives information from one or  
26 more aspects of said host processing environment”), since in that construction Microsoft requires  
27 that the host processing environment include hardware.

28 (2) Microsoft requires that a HPE be within a “VDE node.” The Microsoft definition of

1 VDE incorporates several pages of detailed requirements, none of which is required by the  
2 manner in which HPEs are described in the claim or the specification. Issues regarding whether  
3 VDE should be read into every claim should be resolved in connection with Microsoft's "Global  
4 Construction" argument, discussed above, and should not be "back-doored" into the claims  
5 through the definition of specific terms.

6 (3) Microsoft's definition of "secure" HPE requires software running in "protected  
7 (privileged) mode" and that a non-secure HPE be running in "user mode." The specifications  
8 contain no discussion stating or even implying any such requirement. While the specifications  
9 do discuss processors running in "protected" or "privileged" mode, these discussions have  
10 nothing to do with (and do not mention) HPEs. 16(E), 16(F), 16(G), 16(H).

11 **AA. Derive (Ex. A, Row 92, Ex. B, Row 11, Ex. C, Tab 11).**

12 This is not a term of art and is not specially defined in the specification, in which it is  
13 used in its normal English sense. 11(A), 11(B), 11(C). InterTrust's proposed construction is  
14 based directly on the normal English definition. 11(E).

15 Microsoft defines "derive" to mean "retrieve from a source." That "derive" is not limited  
16 to retrieval from a source is made clear by use of the term in the specification 11(D) and by the  
17 embodiment disclosed for the phrase from 900.155 in which the term "derive" is used, an  
18 embodiment that clearly contemplates generating information. Reiter Decl., ¶ 86. This is plain  
19 English: when one "derives a conclusion," one generates information by the application of  
20 reasoning to facts. One does not simply "retrieve" the conclusion from storage.

21 **BB. Derives information from one or more aspects of said host processing**  
22 **environment (Ex. A, Row 92, Ex. B, Row 29, Ex. C, Tab 29).**

23 InterTrust's construction interprets this phrase in accordance with the plain English  
24 meaning of its words.

25 Microsoft requires that information be derived from the host processing environment  
26 "hardware." No such requirement is imposed by the claim, which specifies merely an "aspect"  
27 of the host processing environment. The disclosed embodiment reveals using software (e.g., the  
28 ROM BIOS, which constitutes software) and stored "information" for this purpose. 29(A);

1 Reiter Decl., ¶¶ 84-85. Moreover, this contradicts Microsoft's definition of host processing  
2 environment, since that definition requires that a host processing environment be made up of  
3 programming, rather than hardware.

4 Microsoft requires that the information "uniquely and persistently" identify the host  
5 processing environment. The claim includes no such requirement, stating only that the  
6 information be derived from "aspects" of the host processing environment, a term used to refer to  
7 features that may disappear. See Aspect, § O, above.

8 **CC. Compares/Comparison (Ex. A, Row 94, Ex. B, Row 5, Ex. C, Tab 5).**

9 These terms are not specially defined in the specification, but are used in accordance with  
10 their normal English meaning. See, e.g., 5(A), 5(B), 5(C), 5(D). InterTrust's definition is based  
11 on that normal meaning.

12 Microsoft attempts to import additional limitations to this term, defining "compare" as  
13 limited to one particular type of microprocessor operation. The specification, however, does not  
14 discuss or even mention any such operation, and uses the word "compare" in its normal English  
15 sense, with no implication that a particular microprocessor operation is contemplated. 5(A),  
16 5(B), 5(C). One of ordinary skill in the art would not understand "compare" to refer to one  
17 particular type of microprocessor operation absent a clear reason to do so. Reiter Decl., 87-89.

18 **DD. Component Assembly (Ex. A, Row 99, Ex. B, Row 6, Ex. C, Tab 6).**

19 InterTrust's proposed definition is taken directly from the manner in which the term is  
20 used in the specification and file history. 6(A), 6(B), 6(K).

21 Microsoft's definition requires that component assemblies be "created by a channel."  
22 The channel mechanism, however, is a preferred embodiment, not a claim element. 6(C).

23 The Microsoft definition requires that a component assembly include load modules.  
24 Although component assemblies may include load modules, the specification describes this as a  
25 preferred embodiment and describes load modules as merely an example of component assembly  
26 components. 6(D), 6(E) (note use of "e.g."), 6(F) (note use of "e.g.").

27 The Microsoft definition requires that a component assembly be assembled and executed  
28 in a Secure Processing Environment. This is directly contradicted by the specification. See 6(B)

1 (component assemblies may be assembled, loaded and executed in either an SPE or an HPE);  
2 6(G) ("certain" component assemblies require a secure execution space). See Protected  
3 Processing Environment (§ P), for an explanation of the differences between the SPE and HPE  
4 embodiments.

5 **EE. Identifying at least one aspect of an execution space required for use and/or**  
6 **execution of the load module (Ex. A, Row 103, Ex. B, Row 30, Ex. C, Tab 30).**

7 InterTrust's definition is based on the plain English meaning of this phrase, including the  
8 separately defined terms. Microsoft incorporates numerous limitations that are inconsistent with  
9 the specification and claims.

10 (1) The Microsoft definition requires that an execution space without "all of those  
11 required aspects" is "incapable of making any such Use (e.g., **Copying**, displaying, printing)  
12 and/or execution of the load module." This implies that, if the execution space lacks these  
13 required aspects but is still capable of making one of the recited uses, the claim element is not  
14 met. The element, however, specifies that the execution space identifier identify an execution  
15 space required for use "and/or" execution of the load module. Thus, if the load module can be  
16 "used" without being "executed," the claim limitation is still met.

17 (2) Microsoft requires that the identifier define "fully, without reference to any other  
18 information." No support exists for this in the claim or the specification, and the disclosed  
19 embodiment is inconsistent with this. Reiter Decl., ¶¶ 91-98.

20 (3) Microsoft's definition includes the following: "used to distinguish it from other  
21 environments of an **execution space**." This phrase has no obvious meaning.

22 //

23 //

24 //

1 VI. CONCLUSION

2 InterTrust's claim constructions rely on the straightforward plain English meaning of the  
3 claim terms, informed by the teachings of the specifications. Microsoft's constructions  
4 contradict the specifications in many respects, and attempt to incorporate numerous limitations  
5 taken directly from preferred embodiments. Moreover, Microsoft's definitions are far longer and  
6 more complex than any patent claim definitions ever adopted by any Court. No jury could  
7 possibly use those definitions in any meaningful way.

8 Microsoft's convoluted and confusing claim constructions are not based on the plain  
9 meanings of the terms, nor on the fundamental legal principles of claim construction. Instead,  
10 Microsoft can only avoid infringement if the InterTrust claims are so loaded up with extraneous  
11 detail that they become impossible to apply to any real world product or process. In doing so,  
12 Microsoft violates fundamental and settled Federal Circuit principles of claim construction,  
13 including the prohibition against reading embodiments from the specifications into the claims.

14 For the reasons set forth above, InterTrust respectfully requests that the Court adopt the  
15 constructions proposed by InterTrust.

16 Dated: March 17, 2003

DERWIN & SIEGEL, LLP

17  
18 By: 

19 DOUGLAS K. DERWIN  
20 Attorneys for Plaintiff  
21 INTERTRUST TECHNOLOGIES  
22 CORPORATION  
23  
24  
25  
26  
27  
28

1 PROOF OF SERVICE

2 I am employed in the City and County of San Francisco, State of California in the office of a  
3 member of the bar of this court at whose direction the following service was made. I am over the  
4 age of eighteen years and not a party to the within action. My business address is Keker & Van  
Nest, LLP, 710 Sansome Street, San Francisco, California 94111.

5 On March 17, 2003, I served the following document(s):

6 INTERTRUST'S OPENING CLAIM CONSTRUCTION BRIEF;

7 DECLARATION OF DOUGLAS K. DERWIN IN SUPPORT OF  
8 INTERTRUST'S OPENING CLAIM CONSTRUCTION BRIEF

9 DECLARATION OF DR. MICHAEL REITER IN SUPPORT OF  
10 INTERTRUST'S CLAIM CONSTRUCTION POSITION

11 DECLARATION OF MICHAEL H. PAGE IN SUPPORT OF  
12 INTERTRUST'S OPENING CLAIM CONSTRUCTION BRIEF

13 ☒ by FEDERAL EXPRESS, by placing a true and correct copy in a sealed envelope addressed as shown  
below. I am readily familiar with the practice of Keker & Van Nest, LLP for correspondence for delivery  
by FedEx Corporation. According to that practice, items are retrieved daily by a FedEx Corporation  
employee for overnight delivery, and by E-MAIL.

14 Eric L Wesenberg, Esq.  
15 Mark R. Weinstein, Esq.  
16 Orrick Herrington & Sutcliffe  
1000 Marsh Road  
Menlo Park, CA 94025  
17 Telephone: 650/614-7400  
Facsimile: 650/614-7401

John D. Vandenberg, Esq.  
James E. Geringer, Esq.  
Kristin L. Cleveland, Esq.  
Klarquist Sparkman Campbell, et al.  
One World Trade Center, Suite 1600  
121 S.W. Salmon Street  
Portland OR 97204  
Telephone: 503/226-7391  
Facsimile: 503/228-9446

18  
19  
20 I declare under penalty of perjury under the laws of the State of California that the above is true  
and correct.

21 Executed on March 17, 2003, at San Francisco, California.

22  
23  
24   
DAWN CURRAN